Attorney's Docket No. 1033048-000049

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Raymond Suorsa et al.	Group Art Unit: 2145
Application No.: 09/838,135	Examiner: TANIM M HOSSAIN
Filed: April 20, 2001	Appeal No.:
For: AUTOMATED PROVISIONING OF COMPUTING NETWORKS USING A NETWORK DATABASE DATA MODEL	

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated June 16, 2005, finally rejecting claims 1, 2 and 4-65, which are reproduced as the Claims Appendix of this brief.

Charge the $250.00 fee under 37 C.F.R. § 41.20(b)(2) to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any other fees under 37 C.F.R. §§1.16, 1.17, 1.21 and 41.20 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Table of Contents

I. Real Party in Interest 1

II. Related Appeals and Interferences 1

III. Status of Claims 1

IV. Status of Amendments 1

V. Summary of Claimed Subject Matter 1

VI. Grounds of Rejection to be Reviewed on Appeal 3

VII. Argument 3

A. Claim 1 3

B. Claims 2, 5-9, 12-15, 58, 59 and 61 5

C. Claims 4, 10, 11, 16-57, 60 and 62-65 6

D. Conclusion 7

VIII. Claims Appendix 7

IX. Evidence Appendix 7

X. Related Proceedings Appendix 8

I. Real Party in Interest

The subject application is assigned to OpsWare, Inc., the successor in interest to LoudCloud, Inc.

II. Related Appeals and Interferences

There are no other prior or pending appeals, interferences, or judicial proceedings which may be related to, directly affect or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. Status of Claims

The application contains claims 1-65. Claim 3 has been canceled. All other claims are currently pending and stand finally rejected. All rejected claims are being appealed.

IV. Status of Amendments

There were no amendments filed subsequent to the final Office Action.

V. Summary of Claimed Subject Matter

The subject application is generally directed to the automated provisioning of devices on a computer network, such as servers that provide the functionality of an Internet web site. Provisioning involves the installation of the software that is executed on the device, and the subsequent configuration of operating parameters of that software to optimize its performance for the intended application. (Specification at paragraph 0005).

A general overview of a provisioning system is provided in Figure 7 of the application. The software to be installed on individual devices is stored in a file system 34. A central database 32 contains the data that is necessary to provision each device, and manages the provisioning process. Communications with the device are carried out by means of a gateway 38. Resident on each device is an agent 36 that conducts the communications with the gateway, as well as executes commands to retrieve, install and configure the software components on its device (paragraphs 0046-0048).

One of the applications of the disclosed system is in the context of a managed services provider which is responsible for provisioning and maintaining servers and other network devices that implement the web sites of multiple customers. See, for example, paragraph 0010. In such a situation, the central filing system 34 may contain a variety of different sets of software that are associated with the different customers. One of the issues that faces the managed services provider, therefore, is to ensure that only the software that is appropriate for a given customer be installed on that customer's servers during a provisioning process. The claimed subject matter is particularly directed to this aspect of the automated provisioning of computer networks.

One example of a procedure that ensures that the proper software is installed on a device is described in paragraphs 0074-0082. Referring to Figure 7, a user may send an instruction to install software on a device, such as Device 1, via a user interface 40. In response to receiving this instruction, the gateway 38 communicates with the agent 36 for Device 1 to inform it of the software to be installed on its device. Upon receiving the information relating to the software to be installed, the agent 36 sends a request to the file server 35 to retrieve the appropriate software. In response, the central file system 34 examines the IP address of Device 1, to determine if the agent 36 is authorized to retrieve the software units that have been requested. In doing so, the central file system communicates with the gateway 38 to query the central database 32 regarding the IP address of Device 1.

A variety of information about devices to be provisioned can be stored in the central database 32 and used to determine whether the requested software is appropriate for the requesting agent's device. Examples of these parameters include the customer account to which the device is assigned, the VLAN with which the device is associated, and the IP address of the device. These factors are used, in turn, to determine whether particular software roles, packages, and/or programs are appropriate for the device on which the command is to be executed. Based upon the information about the device that is retrieved from the central database, a determination is made whether the requested software is appropriate for the device. If so, the file server responds to the request by providing the software to the requesting agent. On the other hand, if the appropriate information about

the device does not reside in the central database 32, the request will be refused.

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action presents two grounds of rejection for review on this appeal:

1. Claims 1, 2, 5-9, 12-15, 58, 59 and 61 stand rejected under 35 U.S.C.§ 102, as being anticipated by the Spencer et al. patent (US 6,633,907);

2. Claims 4, 10, 11, 16-57, 60 and 62-65 stand rejected under 35 U.S.C.§ 103, as being unpatentable over the Spencer patent.

VII. Argument

A. Claim 1

Claim 1 recites a method for the automated provisioning of computer networks. The steps of the claimed method include, among others, those of receiving at least one command to be executed on a network device, and reading parameters from a network database that are related to that network device. Claim 1 further recites the step of "determining whether the at least one command can be properly executed *based upon the parameters read*" (emphasis added).

Claim 1 stands finally rejected under 35 U.S.C. § 102, as being anticipated by the Spencer patent. This patent is directed to the provisioning of online *services* provided by an Internet Service Provider (ISP), such as web hosting, mail, news and chat services (column 1, lines 12-16). It does not pertain to the provisioning of network *devices*, such as servers. Because of its different objective, the Spencer patent does not disclose the claimed subject matter, as discussed hereinafter.

Basically, the Spencer patent discloses the use of service configuration objects (SCOs) to provision and administer user-specified Internet services. There is one SCO associated with each Internet service that can be specified by a user. For instance, Figure 3 illustrates an example in which three SCOs 212, 214 and 216 are respectively associated

with mail, netshow and news services. A data store 218 holds user information that is collected during a provisioning session.

In rejecting claim 1, the final Office Action refers to the Spencer patent at column 8, lines 38-57, and column 9, lines 16-62, as disclosing the step of receiving at least one command to be executed on a network device. These same passages are also cited as disclosing the claimed step of reading of parameters from a network database related to the network device. The first cited passage discloses that the three SCOs are sequentially instantiated and perform the steps required to configure the service with which they are associated before the next SCO is instantiated. The latter passage discloses that, if an error occurs during configuration, a rollback procedure can be carried out, in which each SCO is instructed to perform the reverse operations it performed during configuration, in the reverse order in which the SCOs were instantiated.

Neither of these passages discloses the claimed step of reading parameters from a network database. The term "database" does not even appear in the patent. While the patent discloses a data store 218, that data store does not correspond to the database recited in the claims. In particular, claim 1 recites the step of "reading parameters from a network database *that are related to that network device*" (emphasis added). The data store of the Spencer patent is used to hold information entered by the *user* who is conducting a provisioning session (column 4, lines 8-11; column 6, lines 21-23). The patent gives examples of this type of information as the name, address and billing information for an organization, and the ISP-offered services to which the organization would like to subscribe. See, for example columns 7, lines 48-55. There is no disclosure that the data store provides information about a *device* on which a command is to be executed. In all likelihood, the user is not even aware of the devices that are involved in provisioning the services.

The next step recited in claim 1 is that of "determining whether the at least one command can be properly executed *based upon the parameters read from the database*". The final Office Action again refers to the Spencer patent at column 9, lines 16-62, as allegedly disclosing this claimed step. As noted previously, this portion of the patent discloses that a rollback procedure can be carried out if an error occurs during provisioning of the services. It does not disclose that a determination is made whether a received command

can be properly executed on a network device. Furthermore, it does not disclose that such a determination should be based upon the parameters read from the database, where such parameters relate to the device on which the command is to be executed. As noted above, the information in the data store relates to the transaction that is to be performed to provision a given user's account with desired services. There is no disclosure in the Spencer patent that this information is used to determine whether a received command can be properly executed. The patent does not disclose any nexus between the rollback procedure and information stored in the data store 218.

Accordingly, the Spencer patent does not disclose every element recited in claim 1, and therefore does not anticipate claim 1.

B. Claims 2, 5-9, 12-15, 58, 59 and 61

These claims also stands rejected under 35 U.S.C. § 102 as being anticipated by the Spencer patent. Each claim depends, either directly or indirectly, from claim 1, and therefore cannot be anticipated for at least the reasons set forth in the preceding section of this Brief.

Furthermore, claim 5 depends from claim 4. The rejection of claim 4 (discussed below) acknowledges that this claim is not anticipated by the Spencer patent. As such, any claim that depends from claim 4, and inherently includes all of its elements, likewise cannot be anticipated.

Claim 6 recites that the step of determining whether the command can be properly executed is based on reading software packaging parameters. Claims 8, 9 and 12-15 depend from claim 6 and recite various detailed features of the software packaging parameters. In rejecting claim 6, the final Office Action equates the services disclosed in the Spencer patent with software packages. The Office Action does not identify any support for this position. In any event, even if one were to accept it for the sake of argument, there is still no teaching that a *determination* whether a received command can be executed on a device is based upon reading parameters about the services. There is no disclosure of receiving a command to be executed on a device and making a determination

that such a command can be properly executed on that device, based upon software packaging parameters, or any other kind of information obtained from a database.

Claim 58 recites that the final step of claim 1, namely executing the command on the network device, is limited to entities having an approved access level. Thus, this claim refers to the entity that actually executes the command. Dependent claim 61 recites that this entity is an agent. In rejecting these claims, the final Office Action refers to the Spencer patent's disclosure of security buffering, at column 2, lines 4-6, and column 3, lines 43-54. This disclosure does not have anything to do with the entities that actually execute commands on devices, e.g. SCOs. Rather, it relates to the protection of servers from *users* who do not have authorized access to those servers. The users are not the entities that execute commands on the servers, such as the agents recited in claim 61.

For these additional reasons, therefore, claims 5-9, 12-15, 58, 59 and 61 are not anticipated by the Spencer patent.

C. Claims 4, 10, 11, 16-57, 60 and 62-65

These claims all stand rejected under 35 U.S.C. § 103, in view of the Spencer patent. The final Office Action acknowledges that the Spencer patent does not teach subject matter that is recited in each of these claims. It then goes on to conclude that the missing subject matter would have been obvious to a person of ordinary skill in the art. However, the Office Action fails to provide any support for the allegations.

The rejection of claim 4 is exemplary. This claim recites that steps of receiving a message from a secure provisioning network, and verifying the validity of the message by requesting verification from the secure provisioning network. The final Office Action states:

> Spencer does not specifically teach the requesting of verification of the validity of the message. *It would have been obvious to one of ordinary skill in the art at the time of the invention to include a method to request the validity of a command message.* When commands are given, it must be certain that these commands are coming from the correct place, so as to prevent fraudulent rollbacks and faulty configurations. Including a specific verification scheme would prevent against undue rollbacks and faulty configurations. Including a security measure constitutes a design

choice and therefore does not constitute a patentable distinction. (emphasis added).

The final Office Action does not cite any passages in the Spencer patent that would support this statement. Nor does it cite any other patents that suggest this subject matter.

The three criteria that must be met to establish a prima facie case of obviousness are set forth in MPEP §2143. The third of these criteria is that "the prior art reference... must teach or suggest all the claim limitations." The final Office Action expressly acknowledges that the Spencer patent does not teach subject matter recited in each of the claims rejected under 35 U.S.C. § 103. Since it does not identify any other prior art references that disclose, or otherwise suggest, the claimed elements that are missing from the Spencer patent, it fails to meet at least one of the required criteria for a prima facie case of obviousness.

D. Conclusion

In conclusion, the final Office Action has not shown that the Spencer patent teaches every element of the claims. As such, it does not establish that the Spencer patent anticipates those claims that are rejected under 35 U.S.C. § 102. Furthermore, it has not identified any other prior art teachings that would suggest the claimed elements that are missing from the Spencer patent. Therefore, it fails to meet the criteria for establishing a prima facie case of obviousness that would support a rejection under 35 U.S.C. § 103.

The rejections are not properly founded in the statute, and should be reversed.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

There is no Evidence Appendix for this Brief.

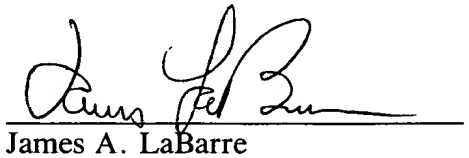
X. Related Proceedings Appendix

There is no Related Proceedings Appendix for this Brief.

Respectfully submitted,

Buchanan Ingersoll PC

Date May 16, 2006

By: 

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. A method for automated provisioning of computer networks, comprising the steps of:

receiving at least one command to be executed on a network device;

reading parameters from a network database related to said network device;

determining whether the at least one command can be properly executed on said network device based upon the parameters read; and

executing the at least one command on said network device only if it is determined that the at least one command can be properly executed.

2. The method of claim 1, wherein the at least one command is executed by an agent on said network device.

4. The method of claim 1, further comprising the steps of:

receiving a message that at least one command is to be executed from a secure provisioning network; and

verifying the validity of the message by requesting verification from the secure provisioning network.

5. The method of claim 4, wherein the step of verifying is accomplished by way of communicating with a communication gateway of the secure provisioning network.

6. The method of claim 1, wherein the step of determining is based on reading software packaging parameters.

7. The method of claim 6, wherein the software packaging parameters comprise compatibility requirements.

8. The method of claim 6, wherein the software packaging parameters comprise software roles.

9. The method of claim 7, wherein the compatibility requirements comprise software roles compatibility requirements.

10. The method of claim 6, wherein the software packaging parameters comprise operating system (OS) parameters.

11. The method of claim 7, wherein the compatibility requirements comprise operating system (OS) compatibility requirements.

12. The method of claim 6, wherein the software packaging parameters comprise parameters regarding specific customer account requirements.

13. The method of claim 7, wherein the compatibility requirements comprise requirements regarding specific customer account compatibility.

14. The method of claim 8, wherein the software roles comprise customer account software roles.

15. The method of claim 9, wherein the software roles compatibility requirements comprise customer account software roles compatibility requirements.

16. The method of claim 6, wherein the software packaging parameters comprise device parameters.

17. The method of claim 16, wherein the device parameters comprise device interface parameters.

18. The method of claim 17, wherein the device interface parameters comprise device internet protocol (IP) address parameters.

19. The method of claim 17, wherein the interface parameters comprise interface type parameters.

20. The method of claim 16, wherein the device parameters comprise interface components parameters.

21. The method of claim 16, wherein the device parameters comprise memory components parameters.

22. The method of claim 16, wherein the device parameters comprise storage components parameters.

23. The method of claim 16, wherein the device parameters comprise central processing unit (CPU) parameters.

24. The method of claim 7, wherein the compatibility requirements comprise device compatibility requirements.

25. The method of claim 24, wherein the device compatibility requirements comprise interface compatibility requirements.

26. The method of claim 25, wherein the interface compatibility requirements comprise IP compatibility requirements.

27. The method of claim 25, wherein the interface compatibility requirements comprise interface type compatibility requirements.

28. The method of claim 24, wherein the device compatibility requirements comprise interface components compatibility requirements.

29. The method of claim 24, wherein the device compatibility requirements comprise memory components compatibility requirements.

30. The method of claim 24, wherein the device compatibility requirements comprise storage components compatibility requirements.

31. The method of claim 24, wherein the device compatibility requirements comprise central processing unit (CPU) components compatibility requirements.

32. The method of claim 8, wherein software roles compatibility requirements comprise device roles compatibility requirements.

33. The method of claim 9, wherein the software roles comprise device roles.

34. The method of claim 6, wherein the software packaging parameters comprise application packaging parameters.

35. The method of claim 7 wherein the compatibility requirements comprise application compatibility requirements.

36. The method of claim 8, wherein the software roles comprise application software roles.

37. The method of claim 36, wherein the application software roles define a group of services.

38. The method of claim 9, wherein the software roles compatibility requirements comprise application roles compatibility requirements.

39. The method of claim 38, wherein the application roles compatibility requirements define a group of services.

40. The method of claim 6, wherein the software packaging parameters relate to a variety of network service tiers.

41. The method of claim 7, wherein the compatibility requirements are defined according to a variety of network service tiers.

42. The method of claim 6, wherein the software packaging parameters are defined by way of configuration parameters.

43. The method of claim 42, wherein the configuration parameters comprise device configuration parameters.

44. The method of claim 42, wherein the configuration parameters comprise interface configuration parameters.

45. The method of claim 42, wherein the configuration parameters comprise virtual IP address parameters.

46. The method of claim 42, wherein the configuration parameters comprise component type parameters.

47. The method of claim 42, wherein the configuration parameters comprise role configuration parameters.

48. The method of claim 47, wherein the role configuration parameters comprise device role configuration parameters.

49. The method of claim 48, wherein the device role configuration parameters comprise device role history configuration parameters.

50. The method of claim 7, wherein the compatibility requirements comprise configuration compatibility requirements.

51. The method of claim 50, wherein the configuration compatibility requirements comprise device configuration compatibility requirements.

52. The method of claim 50, wherein the configuration compatibility requirements comprise interface configuration compatibility requirements.

53. The method of claim 50, wherein the configuration compatibility requirements comprise virtual IP address compatibility requirements.

54. The method of claim 50, wherein the configuration compatibility requirements comprise component type configuration compatibility requirements.

55. The method of claim 50, wherein the configuration compatibility requirements comprise role configuration compatibility requirements.

56. The method of claim 55, wherein the role configuration compatibility requirements comprise device role configuration compatibility requirements.

57. The method of claim 56, wherein the device role configuration compatibility requirements comprise device role history configuration compatibility requirements.

58. The method of claim 1, wherein the step of executing the at least one command is limited to entities having an approved access level to execute the at least one command.

59. The method of claim 58, wherein the access to execute the at least one command is defined in an access control list (ACL).

60. The method of claim 58, wherein the access control list ACL is defined by domain name server (DNS) address of the network device.

61. The method of claim 58, wherein the entity executing the at least one command comprises an agent.

62. The method of claim 61 wherein the access to the agent is limited according to domain name server (DNS) address of the network device.

63. The method of claim 9, wherein the software roles compatibility requirements relate to an IP address of the network device.

64. The method of claim 9, wherein the software roles compatibility requirements relate to IP address compatibility requirements.

65. The method of claim 1, wherein the step of determining is based upon an identification of a virtual local area network (VLAN) with which said network device is associated.